高度なクライアントレス SSL VPN のコンフィギュレーション

Microsoft Kerberos Constrained Delegation ソリューション

Microsoft の Kerberos Constrained Delegation（KCD）は、プライベートネットワーク内の Kerberos で保護された Web アプリケーションへのアクセスを提供します。

Kerberos Constrained Delegation を機能させるために、ASA はソースドメイン（ASA が常駐するドメイン）とターゲットまたはリソースドメイン（Web サービスが常駐するドメイン）間の信頼関係を確立する必要があります。ASA は、サービスにアクセスするリモートアクセスユーザの代わりに、ソースから宛先ドメインへの認証パスを横断し、必要なチケットを取得します。

このように認証パスを越えることは、クロスレルム認証と呼ばれます。クロスレルム認証の各フェーズにおいて、ASA は特定のドメインのクレデンシャルおよび後続ドメインとの信頼関係に依存しています。

KCD の機能

Kerberos は、ネットワーク内のエンティティのデジタル識別情報を検証するために、信頼できる第三者に依存しています。これらのエンティティ（ユーザ、ホストマシン、ホスト上で実行されるサービスなど）は、プリンシパルと呼ばれ、同じドメイン内に存在している必要があります。秘密キーの代わりに、Kerberos では、サーバに対するクライアントの認証にチケットが使用されます。チケットは秘密キーから導出され、クライアントのアイデンティティ、暗号化されたセッション キー、およびフラグで構成されます。各チケットはキー発行局によって発行され、ライフタイムが設定されます。

Kerberos セキュリティ システムは、エンティティ（ユーザ、コンピュータ、またはアプリケーション）を認証するために使用されるネットワーク認証プロトコルであり、情報の受け手として意図されたデバイスのみが復号化できるようにデータを暗号化することによって、ネットワーク伝送を保護します。クライアントレス SSL VPN ユーザに Kerberos で保護された Web サービスへの SSO アクセスを提供するように KCD を設定できます。このような Web サービスやアプリケーションの例として、Outlook Web Access（OWA）、SharePoint、および Internet Information Server（IIS）があります。

Kerberos プロトコルに対する 2 つの拡張機能として、プロトコル移行および制約付き委任が実装されました。これらの拡張機能によって、クライアントレス SSL VPN リモート アクセス ユーザは、プライベート ネットワーク内の Kerberos で認証されるアプリケーションにアクセスできます。

プロトコル移行機能は、ユーザ認証レベルでさまざまな認証メカニズムをサポートし、後続のアプリケーション レイヤでセキュリティ機能（相互認証や制約付き委任など）用に Kerberos プロトコルに切り替えることによって、柔軟性とセキュリティを向上させます。制約付き委任では、ドメイン管理者は、アプリケーションがユーザの代わりを務めることができる範囲を制限することによって、アプリケーション信頼境界を指定して強制適用できます。この柔軟性は、信頼できないサービスによる危険の可能性を減らすことで、アプリケーションのセキュリティ設計を向上させます。

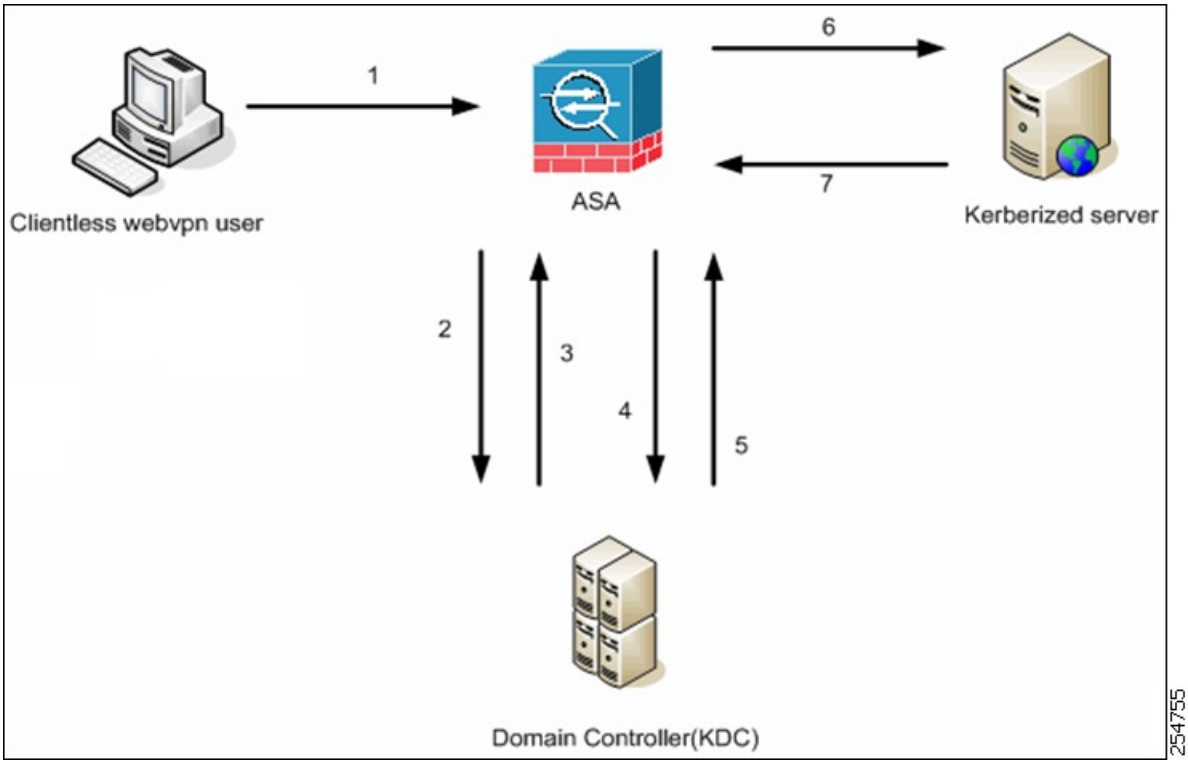
制約付き委任の詳細については、IETF の Web サイト（http://www.ietf.org）にアクセスして、RFC 1510 を参照してください。

KCD の認証フロー

次の図に、委任に対して信頼されたリソースにユーザがクライアントレス ポータルによってアクセスするときに、直接的および間接的に体験するパケットおよびプロセス フローを示します。このプロセスは、次のタスクが完了していることを前提としています。

- ASA 上に設定された KCD
- Windows Active Directory への参加、およびサービスが委任に対して信頼されたことの確認
- Windows Active Directory ドメインのメンバーとして委任された ASA

図 *1 : KCD* プロセス



（注） クライアントレス ユーザ セッションは、ユーザに設定されている認証メカニズムを使用して ASA により認証されます（スマートカード クレデンシャルの場合、ASA はデジタル証明書の userPrincipalName を使用して、Windows Active Directory に対して LDAP 許可を実行します）。

1. 認証が成功すると、ユーザは ASA クライアントレス ポータル ページにログインします。ユーザは、URL をポータル ページに入力するか、ブックマークをクリックして、Web サービスにアクセスします。この Web サービスで認証が必要な場合、サーバは ASA クレデンシャルの認証確認を行い、サーバがサポートしている認証方式のリストを送信します。

（注） クライアントレス SSL VPN の KCD は、すべての認証方式（RADIUS、RSA/SDI、LDAP、デジタル証明書など）に対してサポートされています。次の AAA のサポートに関する表を参照してください。
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492

2. 認証確認時の HTTP ヘッダーに基づいて、ASA はサーバで Kerberos 認証が必要かどうかを判断します（これは SPNEGO メカニズムの一部です）。バックエンド サーバとの接続で Kerberos 認証が必要な場合、ASA は、ユーザに代わって、自身のサービス チケットをキー発行局に要求します。

3. キー発行局は、要求されたチケットを ASA に返します。これらのチケットは ASA に渡されますが、ユーザの許可データが含まれています。ASA は、ユーザがアクセスする特定のサービス用の KCD からのサービスチケットを要求します。

（注） ステップ 1 ～ 3 では、プロトコル移行が行われます。これらのステップの後、Kerberos 以外の認証プロトコルを使用して ASA に対して認証を行うユーザは、透過的に、Kerberos を使用してキー発行局に対して認証されます。

4. ASA は、ユーザがアクセスする特定のサービスのサービスチケットをキー発行局に要求します。
5. キー発行局は、特定のサービスのサービス チケットを ASA に返します。
6. ASA は、サービスチケットを使用して、Web サービスへのアクセスを要求します。
7. Web サーバは、Kerberos サービス チケットを認証して、サービスへのアクセスを付与します。認証が失敗した場合は、適切なエラー メッセージが表示され、確認を求められます。Kerberos 認証が失敗した場合、予期された動作は基本認証にフォールバックします。

制約付き委任用の Kerberos サーバグループの作成

Kerberos Constrained Delegation を使用するには、まず、Kerberos AAA サーバグループを設定する必要があります。サーバグループには、Active Directory（AD）ドメインコントローラが含まれている必要があります。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Microsoft KCD Server]** の順に選択します。

ステップ 2 [Constrained Delegation] ドロップダウンリストの [Kerberos Server Group] の横にある [New] をクリックします。

必要な Kerberos AAA サーバグループが設定済みの場合は、サーバグループを選択するだけで、この手順をスキップできます。

ステップ 3 [Server Group Name] フィールドにグループの名前を入力するか、デフォルトの名前のままにします。

ステップ 4 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバが非アクティブになった場合、そのサーバは、グループの他のすべてのサーバが非アクティブになるまで非アクティブのままとなります。すべてのサーバが非アクティブになると、グループ内のす

べてのサーバが再アクティブ化されます。このアプローチでは、障害が発生したサーバに起因する接続遅延の発生を最小限に抑えられます。

Timedモードでは、障害が発生したサーバは30秒の停止時間の後で再アクティブ化されます。

ステップ 5 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 6 次のサーバを試す前にグループ内の AAA サーバでの AAA トランザクションの失敗の最大数を指定します。

このオプションで設定するのは、応答のないサーバを非アクティブと宣言する前の AAA トランザクションの失敗回数です。

ステップ 7 [Interface Name] で、AD ドメインコントローラへのアクセスに使用できるインターフェイスの名前を選択します。

ステップ 8 グループに追加するドメインコントローラの名前または IP アドレスを入力します。

ステップ 9 サーバへの接続試行のタイムアウト値を指定します。

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the retry interval）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバは非アクティブ化され、ASA は別の AAA サーバ（設定されている場合）への要求の送信を開始します。

ステップ 10 サーバ ポートを指定します。サーバポートは、ポート番号 88、または ASA によって Kerberos サーバとの通信に使用される TCP ポートの番号です。

ステップ 11 再試行間隔を選択します。システムはこの時間待機してから接続要求を再試行します。1 ー 10 秒の範囲で選択できます。デフォルトは 10 秒です。

ステップ 12 Kerberos レルムを設定します。

Kerberos レルム名では数字と大文字だけを使用し、64 文字以内にする必要があります。Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レルムの Active Directory サーバ上で実行する場合は、name の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レルム名です。

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

ASA では、name に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。大文字だけを使用してください。

ステップ 13 [OK] をクリックします。

Kerberos Constrained Delegation（KCD）の設定

次の手順では、Kerberos Constrained Delegation（KCD）を実装する方法について説明します。

始める前に

- ドメインコントローラへのアクセス時に経由するインターフェイスで DNS ルックアップをイネーブルにします。認証委任方式として KCD を使用する場合は、ASA、ドメインコントローラ（DC）、委任しているサービスの間でホスト名解決と通信をイネーブルにするために、DNS が必要です。クライアントレス VPN の配置には、社内ネットワーク（通常は内部インターフェイス）を介した DNS ルックアップが必要です。

  たとえば、**[Configuration]** > **[Device Management]** > **[DNS]** > **[DNS Client]** に移動し、[DNS Lookup] テーブルで内部インターフェイス行の [DNS Enabled] セルをクリックして、[True] を選択します。

- ドメインレルムを DNS ドメインとして使用して、Active Directory（AD）ドメインコントローラを DNS サーバとして使用するように DNS を設定します。

  たとえば、**[Configuration]** > **[Device Management]** > **[DNS]** > **[DNS Client]** に移動し、内部インターフェイスから 10.1.1.10 を [Primary DNS Server] として追加し、EXAMPLE.COM をドメイン名として追加します（サーバグループが複数ある場合は、DefaultDNS サーバグループを選択し、ドメインコントローラを追加します）。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Microsoft KCD Server]** の順に選択します。

ステップ 2 既存の Kerberos AAA サーバグループを選択するか、[New] をクリックして新しいグループを作成します。

新しいグループを作成する場合は、制約付き委任用の Kerberos サーバグループの作成 （4 ページ）を参照してください。

ステップ 3 [Server Access Credentials] で、AD ドメインに参加するために必要なオプションを設定します。

KCD 用に設定されている場合、ASA は Kerberos キーを取得するために、設定されたサーバとの AD ドメイン参加を開始します。これらのキーは、ASA がクライアントレス SSL VPN ユーザに代わってサービスチケットを要求するために必要です。

- [Username]、[Password]：ドメインコントローラで定義された、ドメインに参加するために使用できるユーザ名、およびユーザアカウントのパスワード。ユーザアカウントには、ドメインにデバイスを追加するための管理者権限またはサービスレベル権限が必要です。

ステップ 4 （オプション）必要に応じて、サーバグループ構成の設定を調整します。オプションの説明については、制約付き委任用の Kerberos サーバグループの作成 （4 ページ）を参照してください。

ステップ 5 （オプション）Kerberos サーバグループテーブルでサーバを追加、編集、削除、またはテストします。Kerberos サーバのパラメータについては、制約付き委任用の Kerberos サーバグループの作成 （4 ページ）を参照してください。

Kerberos Constrained Delegation の監視

KCD を監視するには、次のコマンドを使用します。コマンドを入力するには、**[Tools]** > **[Command Line Interface]** または SSH セッションを使用します。

- **show webvpn kcd**

  KCD の構成および参加ステータスを表示します。

```
ciscoasa# show webvpn kcd

KCD state:      Domain Join Complete
Kerberos Realm: EXAMPLE.COM
ADI version:    6.8.0_1252
Machine name:   ciscoasa
ADI instance:   root      1181  1178  0 15:35 ?        00:00:01 /asa/bin/start-adi
Keytab file:    -rw------- 1 root root 79 Jun 16 16:06 /etc/krb5.keytab
```

- **show aaa kerberos** ［**username** *user_id*］

  システム上のキャッシュされた Kerberos チケットを表示します。すべてのチケットを表示することも、特定のユーザのチケットだけを表示することもできます。

```
ASA# show aaa kerberos

Default Principal      Valid Starting        Expires             Service Principal
asa@example.COM        06/29/10 18:33:00     06/30/10 18:33:00
krbtgt/example.COM@example.COM
kcduser@example.COM    06/29/10 17:33:00     06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM    06/29/10 17:33:00     06/30/10 17:33:00
http/owa.example.com@example.COM
```

- **clear aaa kerberos tickets** ［**username** *user_id*］

  システム上のキャッシュされた Kerberos チケットをクリアします。すべてのチケットをクリアすることも、特定のユーザのチケットだけをクリアすることもできます。

外部プロキシ サーバの使用法の設定

[Proxies] ペインを使用して、外部プロキシ サーバによって HTTP 要求と HTTPS 要求を処理するように ASA を設定します。これらのサーバは、ユーザとインターネットの仲介役として機能します。すべてのインターネットアクセスがユーザ制御のサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネットアクセスと管理制御が保証されます。

（注） HTTP および HTTPS プロキシ サービスでは、PDA への接続をサポートしていません。

手順

ステップ 1 [Use an HTTP Proxy Server] をクリックします。

ステップ 2 IP アドレスまたはホスト名で HTTP プロキシ サーバを識別します。

ステップ 3 外部 HTTP プロキシ サーバのホスト名または IP アドレスを入力します。

ステップ 4 HTTP 要求を受信するポートを入力します。デフォルトのポートは 80 です。

ステップ 5 （任意）HTTP プロキシ サーバに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。

- ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。
- **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
- [x-y] は、x から y までの範囲の任意の 1 文字と一致します。x は ANSI 文字セット内のある 1 文字を表し、y は別の 1 文字を表します。
- [!x-y] は、範囲外の任意の 1 文字と一致します。

ステップ 6 （任意）各 HTTP プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。

ステップ 7 各 HTTP 要求とともにプロキシ サーバに送信されるパスワードを入力します。

ステップ 8 HTTP プロキシ サーバの IP アドレスを指定する方法の代替として、[Specify PAC file URL] を選択して、ブラウザにダウンロードするプロキシ自動コンフィギュレーション ファイルを指定できます。ダウンロードが完了すると、PAC ファイルは JavaScript 機能を使用して各 URL のプロキシを識別します。隣接するフィールドに、**http://** を入力し、プロキシ自動設定ファイルの URL を入力します。**http://** の部分を省略すると、ASA はその URL を無視します。

ステップ 9 HTTPS プロキシ サーバを使用するかどうかを選択します。

ステップ 10 クリックして、IP アドレスまたはホスト名で HTTPS プロキシ サーバを識別します。

ステップ 11 外部 HTTPS プロキシ サーバのホスト名または IP アドレスを入力します。

ステップ 12 HTTPS 要求を受信するポートを入力します。デフォルトのポートは 443 です。

ステップ 13 （任意）HTTPS プロキシ サーバに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。

- ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。

- **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
- [x-y] は、x から y までの範囲の任意の 1 文字と一致します。x は ANSI 文字セット内のある 1 文字を表し、y は別の 1 文字を表します。
- [!x-y] は、範囲外の任意の 1 文字と一致します。

ステップ 14 （オプション）各 HTTPS プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、キーワードを入力します。

ステップ 15 各 HTTPS 要求とともにプロキシ サーバに送信されるパスワードを入力します。

クライアントレス SSL VPN セッションでの HTTPS の使用

HTTPS の設定に加えて、Web サイトをプロトコルダウングレード攻撃や cookie ハイジャックから保護するのに役立つ Web セキュリティ ポリシー メカニズムである HTTP Strict-Transport-Security（HSTS）を有効にします。HSTS は、UA およびブラウザを HTTPS Web サイトにリダイレクトし、次のディレクティブを送信することにより指定したタイムアウト期限が切れるまで Web サーバに安全に接続します。

```
http-headers: hsts-server; enable; max-age="31536000"; include-sub-domains; no preload
```

それぞれの説明は次のとおりです。

http-headers：ASA からブラウザに送信されるさまざまな HTTP ヘッダーを設定します。サブモードを設定するか、すべての http-headers 設定をリセットします。

- hsts-client：HSTS クライアントとして機能する HTTP サーバからの HSTS ヘッダーの処理を開始します。
  - enable：HSTS ポリシーを有効または無効にすることができます。有効にすると、既知の HSTS ホストと HSTS ヘッダーに対して HSTS ポリシーが適用されます。
- hsts-server：ASA からブラウザに送信する HSTS ヘッダーを設定します。ASA はヘッダーを基に、HTTP ではなく HTTPS を使用したアクセスのみを許可するようブラウザに指示します。
  - enable：HSTS ポリシーを有効または無効にすることができます。有効にすると、既知の HSTS ホストと HSTS ヘッダーに対して HSTS ポリシーが適用されます。
  - include-sub-domains：ドメイン所有者は、Web ブラウザの HSTS プリロードリストに含める必要があるドメインを送信できます。

（注） HTTPS サイトからの追加リダイレクトを設定するには、（リダイレクト先のページではなく）リダイレクトに HSTS ヘッダーを保持しておく必要があります。

- max-age：（[Enable HSTS] チェックボックスをクリックした後に設定可能）Web サーバが HSTS ホストとして見なされ、HTTPS のみを使用してセキュアにアクセスされる必要のある時間を秒単位で指定します。デフォルトは 3153600 秒（1 年）です。範囲は 0 ～ 2147483647 秒です。
- preload：ブラウザに対し、すでに UA およびブラウザに登録され、HSTS ホストとして取り扱う必要のあるドメインのリストの読み込みを指示します。プリロードされたリストの実装は UA およびブラウザに依存し、各 UA およびブラウザは他のディレクティブの振る舞いに対して追加の制限を指定することができます。たとえば、Chrome のプリロードリストは、HSTS の最大寿命が少なくとも 18 週（10,886,400 秒）であることを指定します。

- x-content-type-options：「X-Content-Type-Options: nosniff」応答ヘッダーの送信を有効にします。
- x-xss-protection：「X-XSS-Protection: 1[; mode=block]」応答ヘッダーの送信を有効にします。
- content-security-policy：ASA からブラウザに WebVPN 接続用の「Content-Security-Policy」ヘッダーを送信することを有効または無効にでき、次のディレクティブを設定できます。
  - default-src：他の CSP ディレクティブのデフォルトソースリストを設定します。ここで、<sources> は URL（または URL のリスト）またはキーワードソース（*self*、*none* など）です。
  - frame-ancestors：ユーザエージェントが、frame、iframe、object、embed、または applet 要素、もしくは HTML 以外のリソースにおける同等の機能を使用したリソースの埋め込みを許可するかどうかを示します。 ここで、<sources> は URL（または URL のリスト）またはキーワードソース（*self*、*none* など）です。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Proxies] の順に選択します。

ステップ 2 ASA からブラウザに送信されるさまざまな HTTP ヘッダーを設定します。

a) 「X-Content-Type-Options: nosniff」応答ヘッダーの送信を有効にする場合にオンにします。
b) 「X-XSS-Protection: 1[; mode=block]」応答ヘッダーの送信を有効にする場合にオンにします。
c) X-XSS-Protection 応答ヘッダーをブロックする場合にオンにします。

ステップ 3 ブラウザの HSTS プリロードリストに含める必要があるドメインを送信するには、[Enable HSTS Server] をクリックします。
[Enable HSTS Subdomains] および [Enable HSTS Preload] が有効になり、HSTS サーバを有効にするとデフォルトで有効になります。

ステップ 4 HSTS の有効時間（秒数）である [HSTS Max Age] を指定します。

値の範囲は <0 ～ 2147483647> 秒です。デフォルトは 31536000 秒（1 年）です。この制限に達すると、HSTS は有効ではなくなります。

HSTS の有効時間（秒数）。値の範囲は <0 ～ 2147483647> 秒です。デフォルトは 31536000 秒（1 年）です。この制限に達すると、HSTS は有効ではなくなります。

ステップ 5 HSTS ホストの HSTS ポリシーの適用を制御し、WebVPN クライアントを処理するには、[Enable HSTS Client] を選択します。

アプリケーション プロファイル カスタマイゼーション フレームワークの設定

クライアントレス SSL に組み込まれているアプリケーション プロファイル カスタマイゼーション フレームワーク（APCF）オプションを使用すると、標準以外のアプリケーションや Web リソースを ASA で処理して、クライアントレス SSL VPN 接続で正常に表示できるようになります。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、何（データ）を変換するかを指定するスクリプトがあります。スクリプトは XML 形式で記述され、sed（ストリーム エディタ）の構文を使用して文字列およびテキストを変換します。

ASA では複数の APCF プロファイルを並行して設定および実行できます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。ASA は、設定履歴に基づいて、最も古いルールを最初に処理し、次に 2 番目に古いルールを処理します。

APCF プロファイルは、ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存できます。

APCF プロファイルは、シスコの担当者のサポートが受けられる場合のみ設定することをお勧めします。

APCF プロファイルの管理

APCF プロファイルは、ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバに保存できます。このペインは、APCF パッケージを追加、編集、および削除する場合と、パッケージを優先順位に応じて並べ替える場合に使用します。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Application Helper] の順に進みます。ここでは、次の機能を実行できます。

- [Add/Edit] をクリックして、新しい APCF プロファイルを作成するか、既存の APCF プロファイルを変更します。

- [Flash file] を選択して、ASA のフラッシュ メモリに保存されている APCF ファイルを指定します。

  次に、[Upload] をクリックして、ローカル コンピュータから ASA のフラッシュ ファイル システムに APCF ファイルを取得するか、[Browse] をクリックして、フラッシュ メモリ内の既存の APCF を選択します。

- [URL] を選択して、HTTP、HTTPS、FTP、または TFTP サーバから APCF ファイルを取得します。

- [Delete] をクリックして、既存の APCF プロファイルを削除します。確認の画面は表示されず、やり直しもできません。
- [Move Up] または [Move Down] をクリックして、リスト内の APCF プロファイルの順序を入れ替えます。順序は、使用される APCF プロファイルを決定します。

ステップ 2 リストに変更が加えられていない場合は、[Refresh] をクリックします。

APCF パッケージのアップロード

手順

ステップ 1 コンピュータ上にある APCF ファイルへのパスが表示されます。[Browse Local] をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。

ステップ 2 APCF ファイルを見つけて、コンピュータに転送するように選択するにはクリックします。[Select File Path] ダイアログボックスに、自分のローカル コンピュータで最後にアクセスしたフォルダの内容が表示されます。APCF ファイルに移動して選択し、[Open] をクリックします。ASDM が [Local File Path] フィールドにファイルのパスを挿入します。

ステップ 3 APCF ファイルをアップロードする ASA 上のパスが [Flash File System Path] に表示されます。[Browse Flash] をクリックして、APCF ファイルをアップロードする ASA 上の場所を特定します。[Browse Flash] ダイアログボックスに、フラッシュ メモリの内容が表示されます。

ステップ 4 ローカル コンピュータで選択した APCF ファイルのファイル名が表示されます。混乱を防ぐために、この名前を使用することをお勧めします。このファイルの名前が正しく表示されていることを確認し、[OK] をクリックします。[Browse Flash] ダイアログボックスが閉じます。ASDM が [Flash File System Path] フィールドにアップロード先のファイル パスを挿入します。

ステップ 5 自分のコンピュータ上の APCF ファイルの場所と、APCF ファイルを ASA にダウンロードする場所を特定したら、[Upload File] をクリックします。

ステップ 6 [Status] ウィンドウが表示され、ファイル転送中は開いたままの状態を維持します。転送が終わり、[Information] ウィンドウに「File is uploaded to flash successfully.」というメッセージが表示されます。[OK] をクリックします。[Upload Image] ダイアログ ウィンドウから、[Local File Path] フィールドと [Flash File System Path] フィールドの内容が削除されます。これは、別のファ

イルをアップロードできることを表します。別のファイルをアップロードするには、上記の手順を繰り返します。それ以外の場合は、[Close] をクリックします。

ステップ 7 [Upload Image] ダイアログ ウィンドウを閉じます。APCF ファイルをフラッシュ メモリにアップロードした後、またはアップロードしない場合に、[Close] をクリックします。アップロードする場合には、[APCF] ウィンドウの [APCF File Location] フィールドにファイル名が表示されます。アップロードしない場合には、「Are you sure you want to close the dialog without uploading the file?」と尋ねる [Close Message] ダイアログボックスが表示されます。ファイルをアップロードしない場合は、[OK] をクリックします。[Close Message] ダイアログボックスと [Upload Image] ダイアログボックスが閉じられ、APCF [Add/Edit] ペインが表示されます。ファイルをアップロードする場合は、[Close Message] ダイアログボックスの [Cancel] をクリックします。ダイアログボックスが閉じられ、フィールドの値がそのままの状態で [Upload Image] ダイアログボックスが再度表示されます。[Upload File] をクリックします。

APCF パケットの管理

手順

ステップ 1 次のコマンドを使用して、APCF パケットを追加、編集、および削除し、パケットを優先順位に応じて並べ替えます。

- [APCF File Location]：APCF パッケージの場所に関する情報を表示します。これは、ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバのいずれかです。
- [Add/Edit]：新規または既存の APCF プロファイルを追加または編集します。
- [Delete]：既存の APCF プロファイルを削除します。確認されず、やり直しもできません。
- [Move Up]：リスト内の APCF プロファイルを再配置します。リストにより、ASA が APCF プロファイルを使用するときの順序が決まります。

ステップ 2 [Flash File] をクリックして、ASA のフラッシュ メモリに保存されている APCF ファイルを指定します。

ステップ 3 フラッシュ メモリに保存されている APCF ファイルのパスを入力します。パスをすでに追加している場合は、そのパスを特定するために参照した後、フラッシュ メモリに格納された APCF ファイルにリダイレクトします。

ステップ 4 [Browse Flash] をクリックして、フラッシュ メモリを参照し、APCF ファイルを指定します。[Browse Flash Dialog] ペインが表示されます。[Folders] および [Files] 列を使用して APCF ファイルを指定します。APCF ファイルを選択して、[OK] をクリックします。ファイルへのパスが [Path] フィールドに表示されます。

（注） 最近ダウンロードしたAPCFファイルの名前が表示されない場合には、[Refresh]をクリックします。

- [Upload]：APCF ファイルをローカル コンピュータから ASA フラッシュ ファイル システムにアップロードします。[Upload APCF Package] ペインが表示されます。
- [URL]：HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存されている APCF ファイルを使用する場合にクリックします。
- [ftp, http, https, and tftp]（ラベルなし）：サーバ タイプを特定します。
- [URL]（ラベルなし）：FTP、HTTP、HTTPS、またはTFTサーバへのパスを入力します。

APCF 構文

APCF プロファイルは、XML フォーマットおよび sed スクリプトの構文を使用します。 次の表に、この場合に使用する XML タグを示します。

APCF のガイドライン

APCF プロファイルの使い方を誤ると、パフォーマンスが低下したり、好ましくない表現のコンテンツになる場合があります。シスコのエンジニアリング部では、ほとんどの場合、APCF プロファイルを提供することで特定アプリケーションの表現上の問題を解決しています。

表 *1 : APCF XML* タグ

タグ	使用目的
<APCF>...</APCF>	すべての APCF XML ファイルを開くための必須のルート要素。
<version>1.0</version>	APCF の実装バージョンを指定する必須のタグ。現在のバージョンは 1.0 だけです。
<application>...</application>	XML 記述の本文を囲む必須タグ。
<id> text </id>	この特定の APCF 機能を記述する必須タグ。
<apcf-entities>...</apcf-entities>	単一または複数の APCF エンティティを囲む必須タグ。

タグ	使用目的
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	これらのタグのうちの 1 つが、コンテンツの種類または APCF 処理が実施される段階を指定します。
<conditions>… </conditions>	処理前および処理後の子要素タグで、次の処理基準を指定します。 • http-version（1.1、1.0、0.9 など） • http-method（get、put、post、webdav） • http-scheme（"http/"、"https/"、その他） • （"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?"）を含む server-regexp 正規表現 • （"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"）を含む server-fnmatch 正規表現 • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • 条件タグのうち2つ以上が存在する場合、ASA はすべてのタグに対して論理 AND を実行します。
<action> … </action>	指定した条件で 1 つ以上のアクションをコンテンツでラップします。これらのアクションを定義するには、次のタグを使用できます（下記参照）。 • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

タグ	使用目的
<do>…</do>	次のいずれかのアクションの定義に使用されるアクション タグの子要素です。 • <no-rewrite/>：リモート サーバから受信したコンテンツを上書きしません。 • <no-toolbar/>：ツールバーを挿入しません。 • <no-gzip/>：コンテンツを圧縮しません。 • <force-cache/>:元のキャッシュ命令を維持します。 • <force-no-cache/>：オブジェクトをキャッシュできないようにします。 • < downgrade-http-version-on-backend>：リモート サーバに要求を送信するときに HTTP/1.0 を使用します。
<sed-script> TEXT </sed-script>	テキストベースのオブジェクトのコンテンツの変更に使用されるアクション タグの子要素です。TEXT は有効な Sed スクリプトである必要があります。<sed-script> は、これより前に定義された <conditions> タグに適用されます。
<rewrite-header></rewrite-header>	アクション タグの子要素です。<header> の子要素タグで指定された HTTP ヘッダーの値を変更します <header>（以下を参照してください）。
<add-header></add-header>	<header> の子要素タグで指定された新しい HTTPヘッダーの追加に使用されるアクション タグの子要素です <header>（以下を参照してください）。
<delete-header></delete-header>	<header> の子要素タグで指定された特定の HTTPヘッダーの削除に使用されるアクション タグの子要素です <header>（以下を参照してください）。

タグ	使用目的

<header></header>	上書き、追加、または削除される HTTP ヘッダー名を指定します。たとえば、次のタグは Connection という名前の HTTP ヘッダーの値を変更します。
	
	`<rewrite-header>`
	`<header>Connection</header>`
	`<value>close</value>`
	`</rewrite-header>`

APCF の設定例

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.example.com</server-fnmatch>
         </conditions>
           <action>
             <do><no-gzip/></do>
           </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>

<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
           <rewrite-header>
                <header>Content-Type</header>
                <value>text/html</value>
           </rewrite-header>
         </action>
      </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

セッションの設定

[Clientless SSL VPN Add/Edit Internal Group Policy] > [More Options] > [Session Settings] ウィンドウでは、クライアントレス SSL VPN のセッションからセッションの間にパーソナライズされ

たユーザ情報を指定できます。デフォルトにより、各グループポリシーはデフォルトのグループポリシーから設定を継承します。このウィンドウを使用して、デフォルトグループポリシーのパーソナライズされたクライアントレス SSL VPN ユーザ情報、およびこれらの設定値を区別するグループ ポリシーすべてを指定します。

手順

ステップ 1 [none] をクリックするか、または [User Storage Location] ドロップダウン メニューからファイル サーバ プロトコル（smb または ftp）をクリックします。シスコでは、ユーザ ストレージに CIFS を使用することを推奨します。ユーザ名/パスワードまたはポート番号を使用せずに CIFS を設定できます。[CIFS] を選択する場合は、次の構文を入力します。

cifs//cifs-share/user/data

[smb] または [ftp] を選択する場合は、次の構文を使用して、隣のテキスト フィールドにファイル システムの宛先を入力します。

username:password@host:port-number/path

次に例を示します。 **mike:mysecret@ftpserver3:2323/public**

（注） このコンフィギュレーションには、ユーザ名、パスワード、および事前共有キーが示されていますが、ASA は内部アルゴリズムにより暗号化した形式でデータを保存し、そのデータを保護します。

ステップ 2 必要な場合は、保管場所へユーザがアクセスできるようにするためにセキュリティ アプライアンスが渡す文字列を入力します。

ステップ 3 [Storage Objects] ドロップダウン メニューから次のいずれかのオプションを選択して、ユーザとの関連でサーバが使用するオブジェクトを指定します。ASA は、これらのオブジェクトを保存してクライアントレス SSL VPN 接続をサポートします。

- cookies,credentials
- cookies
- クレデンシャル

ステップ 4 セッションをタイムアウトするときのトランザクション サイズの限界値を KB 単位で入力します。この属性は、1 つのトランザクションにだけ適用されます。この値よりも大きなトランザクションだけが、セッションの期限切れクロックをリセットします。

エンコーディング

文字エンコーディングは「文字コード」や「文字セット」とも呼ばれ、raw データ（0 や 1 など）を文字と組み合わせ、データを表します。使用する文字エンコード方式は、言語によって決まります。単一の方式を使う言語もあれば、使わない言語もあります。通常は、地域によっ

てブラウザで使用されるデフォルトのコード方式が決まりますが、リモートユーザが変更することもできます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。

エンコード属性によりポータル ページで使用される文字コード方式の値を指定することで、ユーザがブラウザを使用している地域や、ブラウザに対する何らかの変更に関係なく、ページが正しく表示されるようにできます。

デフォルトでは、ASA は「Global Encoding Type」を Common Internet File System（共通インターネット ファイル システム）サーバからのページに適用します。CIFS サーバと適切な文字エンコーディングとのマッピングを、[Global Encoding Type] 属性によってグローバルに、そしてテーブルに示されているファイル エンコーディング例外を使用して個別に行うことにより、ファイル名やディレクトリ パス、およびページの適切なレンダリングが問題となる場合に、CIFS ページが正確に処理および表示できるようにします。

文字エンコーディングの表示または指定

エンコーディングを使用すると、クライアントレス SSL VPN ポータル ページの文字エンコーディングを表示または指定できます。

手順

ステップ 1 [Global Encoding Type] によって、表に記載されている CIFS サーバからの文字エンコーディングを除いて、すべてのクライアントレス SSL VPN ポータル ページが継承する文字エンコーディングが決まります。文字列を入力するか、ドロップダウン リストから選択肢を 1 つ選択します。リストには、最も一般的な次の値だけが表示されます。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis
- unicode
- windows-1252
- none

（注） [none] をクリックするか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

http://www.iana.org/assignments/character-sets で指定されている有効文字セットのいずれかと等しい文字列を、最大 40 文字まで入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されま

せん。ASA の設定を保存するときに、コマンド インタープリタによって大文字が小文字に変換されます。

ステップ 2 エンコーディング要件が「Global Encoding Type」属性設定とは異なる CIFS サーバの名前または IP アドレスを入力します。ASA では、ユーザが指定した大文字と小文字の区別は保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。

ステップ 3 CIFS サーバがクライアントレス SSL VPN ポータル ページに対して指定する必要のある文字エンコーディングを選択します。文字列を入力するか、ドロップダウン リストから選択します。リストには、最も一般的な次の値だけが登録されています。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

  （注） 日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do Not Specify] をクリックして、このフォント ファミリを削除します。

- unicode
- windows-1252
- none

[none] をクリックするか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

http://www.iana.org/assignments/character-sets で指定されている有効文字セットのいずれかと等しい文字列を、最大 40 文字まで入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。ASA の設定を保存するときに、コマンド インタープリタによって大文字が小文字に変換されます。

コンテンツ キャッシングの設定

キャッシュにより、クライアントレス SSL VPN のパフォーマンスを強化します。頻繁に再利用されるオブジェクトをシステム キャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。キャッシュを使用することでトラフィック量が減り、結果として多くのアプリケーションがより効率的に実行されます。

（注） コンテンツ キャッシングをイネーブルにすると、一部のシステムの信頼性が低下します。コンテンツ キャッシングをイネーブルにした後、ランダムにクラッシュが発生する場合は、この機能をディセーブルにしてください。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Content Cache] の順に選択します。

ステップ 2 [Enable Cache] がオフの場合は、オンにします。

ステップ 3 キャッシング条件を定義します。

- [Maximum Object Size]：ASA がキャッシュできるドキュメントの最大サイズを KB 単位で入力します。ASA は、オブジェクトの元のコンテンツ（書き換えまたは圧縮されていないコンテンツ）の長さを測定します。範囲は 0 ～ 10,000 KB で、デフォルトは 1,000 KB です。
- [Minimum Object Size]：ASA がキャッシュできるドキュメントの最小サイズを KB 単位で入力します。ASA は、オブジェクトの元のコンテンツ（書き換えまたは圧縮されていないコンテンツ）の長さを測定します。範囲は 0 ～ 10,000 KB で、デフォルトは 0 KB です。

  （注） [Maximum Object Size] は、[Minimum Object Size] よりも大きい値にする必要があります。

- [Expiration Time]：0 ～ 900 の整数を入力して、オブジェクトを再検証しないでキャッシュする分数を設定します。デフォルトは 1 分です。
- [LM Factor]：1 ～ 100 の整数を入力します。デフォルトは 20 です。
- LM 因数は、最終変更タイムスタンプだけを持つオブジェクトをキャッシュするためのポリシーを設定します。これによって、サーバ設定の変更値を持たないオブジェクトが再検証されます。ASA は、オブジェクトが変更された後の経過時間と、有効期限がコールされた後の経過時間を推定します。推定された期限切れ時刻は、最終変更後の経過時間と LM 因数の積に一致します。LM 因数を 0 に設定すると、ただちに再検証が実行され、100 に設定すると、再検証までの許容最長時間になります。
- この有効期限によって、最終変更タイムスタンプがなく、サーバ設定で有効期限が明示されていないオブジェクトを、ASA がキャッシュする時間の長さを設定します。
- [Cache static content]：たとえば PDF ファイルやイメージなど、リライトされることのないすべてのコンテンツをキャッシュします。
- [Restore Cache Default]：すべてのキャッシュ パラメータをデフォルト値に戻します。

Content Rewrite

[Content Rewrite] ペインには、コンテンツのリライトがイネーブルになっているか、またはオフに切り替わっているすべてのアプリケーションが一覧表示されます。

クライアントレス SSL VPN では、コンテンツ変換およびリライト エンジンによって、JavaScript、VBScript、Java、マルチバイト文字などの高度な要素からプロキシ HTTP へのトラフィックまでを含む、アプリケーション トラフィックを処理します。このようなトラフィックでは、ユーザがアプリケーションにアクセスするのに SSL VPN デバイス内部からアプリケーションを使用しているか、SSL VPN デバイスに依存せずに使用しているかによって、セマンティックやアクセス コントロールのルールが異なる場合があります。

デフォルトでは、セキュリティ アプライアンスはすべてのクライアントレス トラフィックをリライト、または変換します。一部のアプリケーションや Web リソース（公開 Web サイトなど）が ASA を通過しないようにしたい場合があります。そのような場合、ASA では、ASA を通過せずに特定のサイトやアプリケーションをブラウズできるようにするリライト ルールを作成できます。これは、VPN 接続におけるスプリット トンネリングに似ています。

これらの機能強化は、ASA 9.0 の Content Rewriter に行われました。

- コンテンツ リライトは、HTML5 に対するサポートを追加しました。
- クライアントレス SSL VPN リライタ エンジンの品質と有効性が大きく向上しました。その結果、クライアントレス SSL VPN ユーザのエンドユーザ エクスペリエンスも向上が期待できます。

（注） ASA 9.9.2 のコンテンツリライタは、サードパーティのライブラリを使用して HTML と JavaScript を解析する新しい Service Worker ベースのクライアント側リライタです。また、文法ベースのパーサーは、クライアント側でコンテンツの書き換えプロセスを転送するため、ASA のパフォーマンスが向上します。

文法ベースのパーサーには、古いリライタとは異なり、ファイルサイズの制限や複雑さはありません。

クライアント側のリライタは、JavaScript、CSS、および HTML ファイルのみを書き換えることができます。

コンテンツの書き換えが正しく機能するように、次のガイドラインに従ってください。

- ASA とクライアントシステムに有効な SSL 証明書があることを確認します。
- Service Worker およびキャッシュ機能をサポートする Web ブラウザを使用していることを確認します。
  - 拡張コンテンツリライタは、Chrome および Firefox Web ブラウザのみをサポートします。
  - Firefox を使用している場合は、プライベート ブラウジング モードになっていないことを確認します。
- 特定のファイルに適用された *postprocess-response-body* エンティティを持つ Application Profile Customization Framework（APCF）がある場合、ASA はクライアントで APCF をサポートしないため、ファイルはサーバ上で書き換えられます。

コンテンツ書き換えの制限

クライアントレス WebVPN リライタは、実行時に動的に設定されるため、JavaScript ブラケット表記を使用した URL 割り当てを検出できません。

リライト ルールの作成

リライト ルールは複数作成できます。セキュリティ アプライアンスはリライト ルールを順序番号に従って検索するため、ルールの番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

[Content Rewrite] テーブルには、次のカラムがあります。

- [Rule Number]：リスト内でのルールの位置を示す整数を表示します。
- [Rule Name]：ルールが適用されるアプリケーションの名前を付けます。
- [Rewrite Enabled]：コンテンツのリライトをイネーブルかオフで表示します。
- [Resource Mask]：リソース マスクを入力します。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Content Rewrite] の順に移動します。

ステップ 2 [Add] または [Edit] をクリックして、コンテンツ リライト ルールを作成または更新します。

ステップ 3 このルールをイネーブルにするには、[Enable content rewrite] をオンにします。

ステップ 4 このルールの番号を入力します。この番号は、リストの他のルールに相対的に、そのルールの優先順位を示します。番号がないルールはリストの最後に配置されます。有効な範囲は 1 ～ 65534 です。

ステップ 5 （任意） ルールについて説明する英数字を指定します。最大 128 文字です。

ステップ 6 ルールを適用するアプリケーションやリソースに対応する文字列を入力します。文字列の長さは最大で 300 文字です。次のいずれかのワイルドカードを使用できますが、少なくとも 1 つの英数字を指定する必要があります。

- * : すべてに一致します。ASDM では、* または *.* で構成されるマスクは受け付けません。
- ? : 単一文字と一致します。
- [!seq] : シーケンスにない任意の文字と一致します。
- [seq] : シーケンスにある任意の文字と一致します。

コンテンツ リライト ルールの設定例

表 *2:* コンテンツ リライト ルール

機能	コンテンツのリライトをイネーブルにする	ルール番号	ルール名	リソース マスク
youtube.com での HTTP URL のリライタをオフに切り替える	オフ	1	no-rewrite-youtube	*.youtube.com/*
上記のルールに一致しないすべての HTTP URL のリライタをイネーブルにする	Check	65,535	rewrite-all	*

クライアントレス SSL VPN を介した電子メールの使用

Web 電子メールの設定：MS Outlook Web App

ASA は、Microsoft Outlook Web App to Exchange Server 2010 および Microsoft Outlook Web Access to Exchange Server 2013 をサポートしています。

手順

ステップ 1 アドレス フィールドに電子メール サービスの URL を入力するか、クライアントレス SSL VPN セッションでの関連するブックマークをクリックします。

ステップ 2 プロンプトが表示されたら、電子メール サーバのユーザ名を domain\username の形式で入力します。

ステップ 3 電子メール パスワードを入力します。

ブックマークの設定

[Bookmarks] パネルでは、ブックマーク リストを追加、編集、削除、インポート、およびエクスポートできます。

[Bookmarks] パネルを使用して、クライアントレス SSL VPN でアクセスするための、サーバおよび URL のリストを設定します。ブックマーク リストのコンフィギュレーションに続いて、そのリストを 1 つ以上のポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に割り当てることができます。各ポリシーのブックマーク リストは 1 つのみです。リスト名は、各 DAP の [URL Lists] タブのドロップダウン リストに表示されます。

一部の Web ページでの自動サインオンに、マクロ置換を含むブックマークを使用できるようになりました。以前の POST プラグイン アプローチは、管理者がサインオン マクロを含む POST ブックマークを指定し、POST 要求のポストの前にロードするキックオフ ページを受信できるようにするために作成されました。この POST プラグイン アプローチでは、クッキーまたはその他のヘッダー項目の存在を必要とする要求は排除されました。現在は、管理者は事前ロード ページおよび URL を決定し、これによってポスト ログイン要求の送信場所が指定されます。事前ロードページによって、エンドポイント ブラウザは、クレデンシャルを含む POST 要求を使用するのではなく、Web サーバまたは Web アプリケーションに送信される特定の情報を取得できます。

既存のブックマーク リストが表示されます。ブックマーク リストを追加、編集、削除、インポート、またはエクスポートできます。アクセス用のサーバおよび URL のリストを設定し、指定した URL リスト内の項目を配列することができます。

始める前に

ブックマークを設定することでは、ユーザが不正なサイトや会社のアクセプタブル ユース ポリシーに違反するサイトにアクセスすることを防ぐことはできません。ブックマーク リストをグループ ポリシー、ダイナミック アクセス ポリシー、またはその両方に割り当てる以外に、Web ACL をこれらのポリシーに割り当てて、トラフィック フローへのアクセスを制御します。これらのポリシー上の URL エントリをオフに切り替えて、ユーザがアクセスできるページについて混乱しないようにします。

手順

ステップ 1 追加するリストの名前を指定するか、修正または削除するリストの名前を選択します。

ブックマークのタイトルおよび実際の関連付けられた URL が表示されます。

ステップ 2 （任意） [Add] をクリックして、新しいサーバまたは URL を設定します。次のいずれかを追加できます。

- GET または Post メソッドによる URL のブックマークの追加
- 定義済みアプリケーション テンプレートに対する URL の追加
- 自動サインオン アプリケーションへのブックマークの追加

ステップ 3 （任意） [Edit] をクリックして、サーバ、URL、または表示名を変更します。

ステップ 4 （任意） [Delete] をクリックして、選択した項目を URL リストから削除します。確認の画面は表示されず、やり直しもできません。

ステップ 5 （任意） ファイルのインポート元またはエクスポート元の場所を選択します。

- [Local computer]：ローカル PC に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Flash file system]：ASA に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Remote server]：ASA からアクセス可能なリモート サーバに常駐するファイルをインポートする場合にクリックします。
- [Path]：ファイルへのアクセス方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- [Browse Local Files/Browse Flash...]：ファイルのパスを参照します。

ステップ 6 （任意） ブックマークを強調表示して [Assign] をクリックし、選択したブックマークを 1 つ以上のグループ ポリシー、ダイナミック アクセス ポリシー、または LOCAL ユーザに割り当てます。

ステップ 7 （任意） [Move Up] または [Move Down] オプションを使用して、選択した項目の位置を URL リスト内で変更します。

ステップ 8 [OK] をクリックします。

次のタスク

クライアントレス SSL VPN セキュリティ対策について確認してください。

GET または Post メソッドによる URL のブックマークの追加

[Add Bookmark Entry] ダイアログボックスでは、URL リストのリンクまたはブックマークを作成できます。

始める前に

ネットワークの共有フォルダにアクセスするには、\\server\share\subfolder\<personal folder> 形式を使用します。ユーザには、<personal folder> より上のすべてのポイントに対するリスト権限が必要です。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Portal]** > **[Bookmarks]** に移動し、[Add] ボタンをクリックします。

ステップ 2 [URL with GET or POST Method] を選択して、ブックマークの作成に使用します。

ステップ 3 ポータルに表示されるこのブックマークの名前を入力します。

ステップ 4 [URL] ドロップダウン メニューを使用して、URL タイプ（http、https、cifs、または ftp）を選択します。[URL] ドロップダウンは、標準の URL タイプ、インストールしたすべてのプラグインのタイプを示します。

ステップ 5 このブックマーク（URL）の DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符（/?）を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。

server/**?***Parameter*=*Value*&*Parameter*=*Value*

例：

特定のプラグインによって、入力できるオプションのパラメータ/値ペアが決まります。

host/**?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

プラグインに対してシングル サインオンのサポートを指定するには、パラメータ/値ペア **csco_sso=1** を使用します。

ホスト**/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

ステップ 6 （任意）事前ロードURLを入力します。事前ロードURLを入力するときに、待機時間も入力できます。待機時間は、実際のPOSTURLに転送されるまでに、ページのロードに使用できる時間です。

ステップ 7 サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。

ステップ 8 [Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。

ステップ 9 [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。

ステップ 10 ブックマークをクリックして新しいウィンドウで開きます。このウィンドウで、スマート トンネル機能を使用し、ASA を介して宛先サーバとのデータの受け渡しを行います。すべてのブラウザ トラフィックは、SSL VPN トンネルで安全に送受信されます。このオプションでは、ブラウザベースのアプリケーションにスマート トンネルのサポートを提供します。一方で、[Smart Tunnels]（[Clientless SSL VPN] > [Portal] メニューにもあり）では、非ブラウザベースのアプリケーションもスマート トンネル リストに追加し、それをグループ ポリシーとユーザ名に割り当てられます。

ステップ 11 [Allow the Users to Bookmark the Link] をオンにして、クライアントレス SSL VPN ユーザが、ブラウザの [Bookmarks] または [Favorites] オプションを使用できるようにします。選択を解除すると、これらのオプションを使用できません。このオプションをオフにすると、クライアントレス SSL VPN ポータルの [Home] セクションにブックマークは表示されません。

ステップ 12 （任意） [Advanced Options] を選択して、ブックマークの特徴の詳細を設定します。

- [URL Method]：単純なデータ取得の場合には [Get] を選択します。データの保存または更新、製品の注文、電子メールの送信など、データを処理することによってデータに変更が加えられる可能性がある場合には、[Post] を選択します。
- [Post Parameters]：Post URL 方式の詳細を設定します。

定義済みアプリケーション テンプレートに対する URL の追加

このオプションは、事前に定義された ASDM テンプレートを選択しているユーザのブックマークの作成を簡略化します。ASDM テンプレートには、特定の明確に定義されたアプリケーションに対する事前に入力された必要な値が含まれます。

始める前に

定義済みアプリケーション テンプレートは、次のアプリケーションで現在使用できます。

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010

- Microsoft SharePoint 2013

手順

ステップ 1 ユーザに対して表示するブックマークの名前を入力します。

ステップ 2 サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。

ステップ 3 [Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。

ステップ 4 [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。

ステップ 5 （任意） [Place This Bookmark on the VPN Home Page] チェックボックスをオンにします。

ステップ 6 [Select Auto Sign-on Application] リストで、必要なアプリケーションをクリックします。使用可能なアプリケーションは次のとおりです。

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

ステップ 7 ログイン ページの前にロードされるページの URL を入力します。このページには、ログイン画面に進むためのユーザ インタラクションが必要になります。URL には、任意の数の記号を置き換える * を入力できます（たとえば、http*://www.example.com/test）。

ステップ 8 [Pre-login Page Control ID] を入力します。これは、ログイン ページに進む前に事前ログイン ページの URL でクリック イベントを取得する制御/タグの ID です。

ステップ 9 [Application Parameters] を入力します。アプリケーションに応じて、次の内容が含まれる可能性があります。

- プロトコル。HTTP または HTTPS。
- ホスト名。たとえば、www.cisco.com などです。
- ポート番号。アプリケーションで使用されるポート。
- [URL Path Appendix]。たとえば、/Citrix/XenApp などです。通常これは、自動入力されます。
- [Domain]。接続するドメイン。

- [User Name]。ユーザ名として使用する SSL VPN 変数。[Select Variable] をクリックして、異なる変数を選択します。
- パスワード。パスワードとして使用する SSL VPN 変数。[Select Variable] をクリックして、異なる変数を選択します。

ステップ 10 （任意）[Preview] をクリックして、テンプレートの出力を表示します。[Edit] をクリックすると、テンプレートを変更できます。

ステップ 11 [OK] をクリックして、変更を行います。または、[Cancel] をクリックして変更を破棄します。

自動サインオン アプリケーションのブックマークの追加

このオプションでは、複雑な自動サインオン アプリケーションのブックマークを作成できます。

自動サインオン アプリケーションの設定には、2 つの手順が必要になります。

1. 基本的な初期データがあり、POST パラメータがないブックマークを定義します。ブックマークを保存および割り当てて、グループまたはユーザ ポリシーで使用します。
2. ブックマークを再度編集します。特定のキャプチャ機能を使用して、SSL VPN パラメータをキャプチャし、ブックマークで編集します。

手順

ステップ 1 ユーザに対して表示するブックマークの名前を入力します。

ステップ 2 [URL] ドロップダウン メニューを使用して、URL タイプ（http、https、cifs、または ftp）を選択します。インポートされたすべてのプラグインの URL タイプが、このメニューに表示されます。ポータル ページにリンクとしてプラグインを表示するには、プラグインの URL タイプを選択します。

ステップ 3 ブックマークの DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符（/?）を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。

server/**?***Parameter*=*Value*&*Parameter*=*Value*

例：

たとえば、入力できるオプションのパラメータ/値ペアは、特定のプラグインによって決まります。

```
host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```

プラグインに対して、シングル サインオン サポートを提供するには、パラメータ/値ペア **csco_sso=1** を使用します。

```
host/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```

ステップ 4 サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。

ステップ 5 [Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。

ステップ 6 [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。

ステップ 7 （任意） [Place This Bookmark on the VPN Home Page] チェックボックスをオンにします。

ステップ 8 [Login Page URL] を入力します。入力する URL には、ワイルドカードを使用できます。たとえば、http*://www.example.com/myurl* と入力します。

ステップ 9 [Landing Page URL] を入力します。ASA では、アプリケーションへの正常なログインを検出するために、ランディング ページを設定する必要があります。

ステップ 10 （任意） [Post Script] を入力します。Microsoft Outlook Web Access などの一部の Web アプリケーションは、JavaScript を実行して、ログイン フォームを送信する前に、要求パラメータを変更する場合があります。[Post Script] フィールドでは、このようなアプリケーションの JavaScript を入力できます。

ステップ 11 必要な [Form Parameters] を追加します。必要な SSL VPN 変数ごとに、[Add] をクリックして [Name] を入力し、リストから変数を選択します。パラメータを変更するには [Edit] をクリックし、削除するには [Delete] をクリックします。

ステップ 12 ログイン ページの前にロードされるページの URL を入力します。このページには、ログイン画面に進むためのユーザ インタラクションが必要になります。URL には、任意の数の記号を置き換える * を入力できます（たとえば、http*://www.example.com/test）。

ステップ 13 [Pre-login Page Control ID] を入力します。これは、ログイン ページに進む前に事前ログイン ページの URL でクリック イベントを取得する制御/タグの ID です。

ステップ 14 [OK] をクリックして、変更を行います。または、[Cancel] をクリックして変更を破棄します。

次の作業

次のタスク

ブックマークを編集する場合、HTML Parameter Capture 機能を使用して、VPN 自動サインオン パラメータをキャプチャできます。ブックマークは保存され、グループ ポリシーまたはユーザにまず割り当てられる必要があります。

[SSL VPN Username] を入力してから、[Start Capture] をクリックします。次に、Web ブラウザを使用して、VPN セッションを開始して、イントラネットのページに進みます。プロセスを完了するには、[Stop Capture] をクリックします。パラメータが編集できるようになり、ブックマークに挿入されます。

ブックマーク リストのインポートおよびエクスポート

すでに設定済みのブックマーク リストは、インポートまたはエクスポートできます。使用準備ができているリストをインポートします。リストをエクスポートして修正または編集してから、再インポートすることもできます。

手順

ステップ 1 ブックマーク リストを名前で指定します。最大 64 文字で、スペースは使用できません。

ステップ 2 リスト ファイルをインポートする、またはエクスポートするための方法を選択します。

- [Local computer]：ローカル PC に常駐するファイルをインポートする場合に選択します。
- [Flash file system]：ASA に常駐するファイルをエクスポートする場合に選択します。
- [Remote server]：ASA からアクセス可能なリモート サーバに常駐する URL リスト ファイルをインポートする場合にクリックします。
- [Path]：ファイルへのアクセス方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- [Browse Local Files/Browse Flash]：ファイルのパスを参照します。
- [Import/Export Now]：リスト ファイルをインポートまたはエクスポートします。

Import and Export GUI Customization Objects (Web Contents)

このダイアログボックスでは、Web コンテンツ オブジェクトをインポートおよびエクスポートできます。Web コンテンツ オブジェクトの名前とファイル タイプが表示されます。

Web コンテンツには、全体的に設定されたホーム ページから、エンド ユーザ ポータルをカスタマイズするときに使用するアイコンやイメージまで、さまざまな種類があります。設定済みの Web コンテンツは、インポートまたはエクスポートできます。使用準備ができている Web コンテンツをインポートします。Web コンテンツをエクスポートして修正または編集してから、再インポートすることもできます。

手順

ステップ 1 ファイルのインポート元またはエクスポート元の場所を選択します。

- [Local computer]：ローカル PC に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Flash file system]：ASA に常駐するファイルをインポートまたはエクスポートする場合にクリックします。

- [Remote server]：ASA からアクセス可能なリモート サーバに常駐するファイルをインポートする場合にクリックします。
- [Path]：ファイルへのアクセス方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- [Browse Local Files.../Browse Flash...]：ファイルのパスを参照します。

ステップ 2 コンテンツへのアクセスに認証が必要かどうかを決定します。

パスのプレフィックスは、認証を要求するかどうかに応じて異なります。ASA は、認証が必要なオブジェクトの場合には /+CSCOE+/ を使用し、認証が不要なオブジェクトの場合には /+CSCOU+/ を使用します。ASA では、/+CSCOE+/ オブジェクトはポータル ページにのみ表示されますが、/+CSCOU+/ オブジェクトはログイン ページまたはポータル ページで表示したり使用することができます。

ステップ 3 クリックして、ファイルをインポートまたはエクスポートします。

POST パラメータの追加および編集

このペインでは、ブックマーク エントリと URL リストのポスト パラメータを設定します。

クライアントレス SSL VPN 変数により、URL およびフォームベースの HTTP post 操作で置換が実行できます。これらの変数はマクロとも呼ばれ、ユーザ ID とパスワード、またはその他の入力パラメータを含む、パーソナル リソースへのユーザ アクセスを設定できます。このようなリソースの例には、ブックマーク エントリ、URL リスト、およびファイル共有などがあります。

手順

ステップ 1 パラメータの名前と値を、対応する HTML フォームのとおりに指定します。たとえば、

<input name="*param_name*" value="*param_value*"> です。

提供されている変数のいずれかをドロップダウン リストから選択できます。また、変数を作成できます。ドロップダウン リストからは、次の変数を選択します。

表 *3:* クライアントレス *SSL VPN* の変数

No.	変数置換	定義
1	CSCO_WEBVPN_USERNAME	SSL VPN ユーザ ログイン ID。
2	CSCO_WEBVPN_PASSWORD	SSL VPN ユーザ ログイン パスワード。

No.	変数置換	定義
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN ユーザ内部リソース パスワード。キャッシュされた認定証であり、AAA サーバによって認証されていません。ユーザがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN ユーザ ログイン グループ ドロップダウン、接続プロファイル内のグループ エイリアス
5	CSCO_WEBVPN_MACRO1	RADIUS/LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。 RADIUS経由での変数置換は、VSA#223 によって行われます。
6	CSCO_WEBVPN_MACRO2	RADIUS/LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。 RADIUS経由での変数置換は、VSA#224 によって行われます。
7	CSCO_WEBVPN_PRIMARY_USERNAME	二重認証用のプライマリ ユーザのログイン ID
8	CSCO_WEBVPN_PRIMARY_PASSWORD	二重認証用のプライマリ ユーザのログイン パスワード

No.	変数置換	定義
9	CSCO_WEBVPN_SECONDARY_USERNAME	二重認証用のセカンダリ ユーザのログイン ID
10	CSCO_WEBVPN_SECONDARY_PASSWORD	二重認証用のセカンダリ ユーザのログイン ID
11	CSCO_WEBVPN_DYNAMIC_URL	ユーザのポータルで複数のブックマーク リンクを生成できる単一のブックマーク。
12	CSCO_WEBVPN_MACROLIST	静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。

ASA はこれら 6 つの変数文字列のいずれかをエンドユーザ要求（ブックマークまたはポストフォーム）で認識すると、リモート サーバに要求を渡す前に、変数をユーザ固有の値に置換します。

（注） プレーン テキストで（セキュリティ アプライアンスを使用せずに）HTTP Sniffer トレースを実行すると、任意のアプリケーションの http-post パラメータを取得できます。次のリンクから、無料のブラウザ キャプチャ ツールである HTTP アナライザを入手できます。http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe

ステップ 2 該当する変数を選択するには、次の注意事項に従ってください。

- 変数 1 ～ 4 を使用する。ASA は、[SSL VPN Login] ページから最初の 4 つの置き換えの値を取得します。値には、ユーザ名、パスワード、内部パスワード（オプション）、およびグループのフィールドが含まれています。ユーザ要求内のこれらのストリングを認識し、このストリングをユーザ固有の値で置き換えてから、リモート サーバに要求を渡します。

```
For example, if a URL list contains the link,
http://someserver/homepage/CSCO_WEBVPN_USERNAME.html, the ASA translates it to the
following unique links:

For USER1, the link becomes http://someserver/homepage/USER1.html

For USER2, the link is http://someserver/homepage/USER2.html

In the following case, cifs://server/users/CSCO_WEBVPN_USERNAME lets the ASA map a
file drive to specific users:
For USER1, the link becomes cifs://server/users/USER1
For USER 2, the link is cifs://server/users/USER2
```

- 変数 5 と 6 を使用する。マクロ 5 および 6 の値は、RADIUS または LDAP のベンダー固有属性（VSA）です。これらにより、RADIUS または LDAP サーバのいずれかで設定した代わりの設定を使用できるようになります。

- 変数 7 ～ 10 を使用する。ASA はこれら 4 つの変数文字列のいずれかをエンドユーザ要求（ブックマークまたはポスト フォーム）で認識すると、リモート サーバに要求を渡す前に、変数をユーザ固有の値に置換します。

```
The following example sets a URL for the homepage:
WebVPN-Macro-Value1 (ID=223), type string, is returned as wwwin-portal.example.com
WebVPN-Macro-Value2 (ID=224), type string, is returned as 401k.com

To set a home page value, you would configure the variable substitution as
https://CSCO_WEBVPN_MACRO1, which would translate to https://wwwin-portal.example.com.
```

- 変数 11 を使用する。これらのブックマークは、CSCO_WEBVPN_DYNAMIC_URL がマッピングされている LDAP 属性マップに基づいて生成されます。LDAP から受信した文字列は、デリミタ パラメータを使用して解析され、値のリストになります。この変数を url フィールドで使用したり、ブックマーク内で POST パラメータとして使用すると、解析された LDAP 文字列の各値に対してブックマークが生成されます。CSCO_WEBVPN_DYNAMIC_URL を使用するブックマークの設定例を以下に示します。

```
<bookmark>
    <title>Test Bookmark</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://CSCO_WEBVPN_DYNAMIC_URL1(".")</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url></login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <<post-param>
        <value>value1</value>
        <name>parameter1</name>
    </post-param>
</bookmark>
```

CSCO_WEBVPN_DYNAMIC_URL は LDAP 属性マップに設定されており、host1.cisco.com、host2.cisco.com、host3.cisco.com に対応しています。デリミタに従って、http://host1.cisco.com、http://host2.cisco.com、http://host3.cisco.com を含む単一のコンフィギュレーションから生成された、3 つの個別の URL と 3 つのブックマークを取得できます。

さらに、POST パラメータの一部として次のマクロを使用できます。

```
<bookmark>
    <title>Test Bookmark</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://www.myhost.cisco.com</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url></login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <post-param>
        <value>CSCO_WEBVPN_DYNAMIC_URL(";")</value>
```

```
        <name>host</name>
    </bookmark>
```

同じマッピングされたLDAP属性を使用して、ターゲットURL http://www.myhost.cisco.com を含む3つのブックマークが作成されます。それぞれのブックマークは異なるPOSTパラメータと、名前 *host* および値 host1.cisco.com、host2.cisco.com、host3.cisco.com を持ちます。

（注） CSCO_WEBVPN_DYNAMIC_URL はブックマークでのみ使用できます。マクロをサポートしている別の箇所（Citrix Mobile Receiver の vdi CLI コンフィギュレーションなど）で使用することはできません。外部ポータルページを定義するために使用することもできません。

- 変数 12 を使用する。このマクロは入力として 3 つのパラメータ（インデックス、デリミタ、エスケープ）を取ります。インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。デリミタは管理者によって提供される文字列です。この文字列の文字を使用してLDAPにマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに1つのデリミタが使用されます。エスケープは、ASA要求に置き換える前に LDAP 文字列に適用する条件選択肢です。

  たとえば、CSCO_WEBVPN_MACROLIST(2, ",", url-encode) は、リストの 2 番目の値を使用すること、および区切り文字として単一のカンマを使用して文字列を区切り、リストにすることを指定しています。値は、バックエンドへの ASA 要求に置換されるときに符号化された URL になります。エスケープ ルーチンには、次の値が使用されます。

  - *None*：バックエンド サーバへの送信前に、文字列値に対して変換を行いません。
  - *url-code*：解析された各値は符号化されたURLになります。ただし、URLで特殊文字列を構成する一連の予約文字は除外されます。
  - *url-encode-data*：解析された各値は、URL エンコードで完全に変換されます。
  - *base64*：解析された各値は Base 64 で符号化されます。

  CSCO_WEBVPN_MACROLIST1 を使用するブックマークの設定例を以下に示します。

```
<bookmark>
    <title>MyHost</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://www.myhost.cisco.com</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url><login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <post-param>
        <value>CSCO_WEBVPN_MACROLIST1(1, ";", url-encode-data)>/value>
        <name>param1</name>
        <value>CSCO_WEBVON_MACROLIST1(2, ";", url-encode-data)</value>
        <name>param2</name>
        <value>CSCO_WEBVPN_MACROLIST1(3, ";", url-encode-data)</value>
        <name>param3</name>
```

```
    </post-param>
</bookmark>
```

このブックマークを使用すると、www.myhost.cisco.com をブラウズして、3 つの POST パラメータ（param1、param2、param3）を自動的にサーバに送信できます。ASA は、CSCO_WEBVPN_MACROLIST1 の値をパラメータに置換してから、バックエンドに送信します。

（注） CSCO_WEBVPN_MACROLIST は、他のマクロが使用される箇所ならどこでも使用できます。

- この場合の最善の方法は、ASDM で Homepage URL パラメータを設定することです。スクリプトを記述したり何かをアップロードしなくても、管理者はグループ ポリシー内のどのホームページがスマート トンネル経由で接続するかを指定できます。ASDM の Network Client SSL VPN または Clientless SSL VPN Access セクションから、[Add/Edit Group Policy] ペインに移動します。パスは次のとおりです。
  - [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit Group Policy] > [Advanced] > [SSL VPN Client] > [Customization] > [Homepage URL] 属性
  - [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit Group Policy] > [More Options] > [Customization] > [Homepage URL] 属性

ステップ 3 ブックマークまたは URL エントリを設定します。SSL VPN 認証で RSA ワンタイム パスワード（OTP）を使用し、続いて OWA 電子メール アクセスでスタティックな内部パスワードを使用することによって、HTTP Post を使用して OWA リソースにログインできます。この場合の最善の方法は、次のパスのいずれかを使用して ASDM でブックマーク エントリを追加または編集することです。

- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] > [Add/Edit Bookmark Lists] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters]（URL Method 属性の [Post] をクリックすると表示されます）
- [Network (Client) Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [URL Lists] タブ > [Manage] ボタン > [Configured GUI Customization Objects] > [Add/Edit] ボタン > [Add/Edit Bookmark List] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters]

ステップ 4 ファイル共有（CIFS）URL 置換を設定することによって、より柔軟なブックマーク設定を構成します。URL「cifs://server/CSCO_WEBVPN_USERNAME」を設定すると、ASA はそれをユーザのファイル共有ホームディレクトリに自動的にマッピングします。この方法では、パスワードおよび内部パスワード置換も行えます。次に、URL 置換の例を示します。

```
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

外部ポートのカスタマイズ

事前設定されたポータルを使用する代わりに、外部ポータル機能を使用して独自のポータルを作成できます。独自のポータルを設定する場合、クライアントレス ポータルをバイパスし、POST 要求を送信してポータルを取得できます。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Portal]** > **[Customization]** を選択します。必要なカスタマイゼーションを強調表示し、[Edit] を選択します。

ステップ 2 [Enable External Portal] チェックボックスをオンにします。

ステップ 3 [URL] フィールドに、POST 要求が許可されるように、必要な外部ポータルを入力します。